II COMMISSIONE PERMANENTE

(Giustizia)

S O M M A R I O

AUDIZIONI INFORMALI

Martedì 13 luglio 2021.

Audizione informale, in videoconferenza, di Luisa Betti Dakli, Direttrice di DonnexDiritti Network e di International Women, e di Elisabetta Rampelli, Presidente dell'Unione italiana forense, nell'ambito dell'esame delle proposte di legge C. 2102 Bazoli, C. 2264 Locatelli, C. 2796 Bellucci, C. 2897 Ascari, C. 2937 Giannone e C. 3148 Boldrini, recanti modifiche al codice civile e alla legge 4 maggio 1983, n. 184, in materia di affidamento dei minori.

L'audizione informale è stata svolta dalle 13.30 alle 14.35.

SEDE CONSULTIVA

Martedì 13 luglio 2021. — Presidenza del presidente Mario PERANTONI. — Interviene, in videoconferenza, il sottosegretario di Stato per la giustizia Francesco Paolo Sisto.

La seduta comincia alle 14.35.

Sui lavori della Commissione.

Mario PERANTONI, *presidente*, avverte che, poiché nelle sedute odierne non sono previste votazioni, ai deputati è consentita la partecipazione da remoto, in videoconferenza, secondo le modalità stabilite dalla Giunta per il Regolamento nella riunione del 4 novembre 2020.

DL 82/2021: Disposizioni urgenti in materia di cybersicurezza, definizione dell'architettura nazionale di cybersicurezza e istituzione dell'Agenzia per la cybersicurezza nazionale.

C. 3161 Governo.

(Parere alle Commissioni riunite I e IX).

(Esame e rinvio).

La Commissione inizia l'esame del provvedimento in oggetto.

Mario PERANTONI (M5S), *presidente*, passa all'illustrazione del provvedimento in esame, in sostituzione del relatore, onorevole Paolini, impossibilitato a partecipare alla seduta odierna. Rammenta in primo luogo che il provvedimento, in considerazione dell'accresciuta esposizione alle minacce cibernetiche che ha imposto nell'agenda nazionale ed internazionale la necessità di sviluppare, in tempi brevi, idonei e sempre più stringenti meccanismi di tutela, aggiorna l'architettura nazionale di sicurezza cibernetica. Ricorda a tale proposito che la cornice legislativa delle misure da adottare per la sicurezza delle reti e dei sistemi informativi è dettata dal decreto legislativo 18 maggio 2018, n. 65, con il quale l'Italia ha recepito nell'ordinamento nazionale la direttiva (UE) 2016/1148 del 6 luglio 2016, la quale reca misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione (cosiddetta direttiva NIS – *Network and Information Security*). Successivamente, il decreto-legge 21 settembre 2019, n. 105, è intervenuto in materia, attraverso l'istituzione di un perimetro di sicurezza nazionale cibernetica e la previsione di misure volte a garantire i necessari standard di sicurezza rivolti a minimizzare i rischi.

Segnala inoltre che la sicurezza cibernetica costituisce uno degli interventi previsti dal Piano nazionale di ripresa e resilienza (PNRR) trasmesso dal Governo alla Commissione europea il 30 aprile 2021, nell'ambito della Missione 1 « Digitalizzazione, innovazione, competitività, cultura e turismo ». All'investimento, volto alla creazione ed al rafforzamento delle infrastrutture legate alla protezione cibernetica del Paese, sono destinati circa 620 milioni di euro di cui 241 milioni di euro per la creazione di una infrastruttura nazionale, 231 milioni di euro per il rafforzamento delle principali strutture operative del perimetro di sicurezza nazionale cibernetica, 150 milioni di euro per il rafforzamento delle capacità nazionali di difesa informatica presso i Ministeri dell'interno, della difesa e della giustizia, la Guardia di Finanza e il Consiglio di Stato.

Come è già avvenuto anche in altri Paesi (Francia, Germania e Regno Unito), il decreto in esame provvede dunque a istituire un'Agenzia nazionale di cybersicurezza a cui attribuire direttamente la responsabilità delle attività di sicurezza informatica, concentrando in essa le funzioni specialistiche in materia, ad esclusione di quelle attinenti alla cyber-intelligence (di competenza degli organismi di informazione per la sicurezza), alla cyber-defense (intesa come difesa e sicurezza militare dello Stato, di competenza del Ministero della difesa) e alla prevenzione e repressione dei reati (di competenza delle Forze di polizia).

In estrema sintesi, il provvedimento, che è costituito da 19 articoli, provvede: a definire le competenze in materia di cybersicurezza; a razionalizzare le competenze in materia di cybersicurezza attualmente attribuite ad una pluralità di soggetti istituzionali; a supportare lo sviluppo di capacità industriali, tecnologiche e scientifiche nel campo della cybersicurezza, in un'ottica di autonomia strategica nazionale ed europea nel settore; a dare attuazione al Piano Nazionale di Ripresa e Resilienza (PNRR); a mettere in stretto raccordo l'architettura di cybersicurezza nazionale con il Sistema di informazione per la sicurezza della Repubblica previsto dalla legge 3 agosto 2007, n. 124, a fronte di una chiara separazione di competenze a tutela della sicurezza nazionale nel dominio cibernetico e dell'attribuzione di poteri di controllo al Comitato parlamentare per la sicurezza della Repubblica (Copasir); a promuovere una gestione coordinata, con i diversi attori coinvolti, delle attività di prevenzione, preparazione e risposta a situazioni di crisi, anche mediante la costituzione, nell'ambito dell'istituenda Agenzia, del Nucleo per la cybersicurezza.

Nel rinviare alla documentazione predisposta dagli uffici per una dettagliata descrizione dei contenuti del provvedimento, in questa sede si limita ad illustrare i profili di competenza della Commissione Giustizia.

A tal fine segnala in primo luogo che l'articolo 4 istituisce, presso la Presidenza del Consiglio dei ministri, il Comitato interministeriale per la cybersicurezza (CIC), organismo con funzioni di consulenza, proposta e vigilanza in materia di politiche di cybersicurezza, anche ai fini della tutela della sicurezza nazionale nello spazio cibernetico, di cui fa parte tra gli altri anche il Ministro della Giustizia. Evidenzia a tale proposito che, analogamente, un rappresentante del Ministro della Giustizia fa parte anche del Nucleo per la cybersicurezza, presieduto dal direttore generale dell'Agenzia e previsto dall'articolo 8 quale supporto del Presidente del Consiglio riguardo alle tematiche della cybersicurezza, per gli aspetti relativi alla prevenzione e preparazione ad eventuali situazioni di crisi e per l'attivazione delle procedure di allertamento.

Segnala inoltre che l'articolo 7 determina le funzioni della futura Agenzia per la cybersicurezza nazionale, cui viene attribuita la qualifica di Autorità nazionale, ai fini del complesso di relazioni e funzioni disegnato dalle norme europee ed interne. In tale quadro, l'Agenzia predispone in primo luogo la strategia nazionale di cybersicurezza; assume compiti finora attribuiti a diversi soggetti quali il Ministero dello sviluppo economico, la Presidenza del Consiglio, il Dipartimento delle informazioni e della sicurezza e l'Agenzia per l'Italia digitale; promuove iniziative per lo sviluppo di competenze e capacità. In particolare, ai sensi della lettera *e)* del comma 1 dell'articolo 7, l'Autorità nazionale di certificazione della cybersicurezza, con riguardo a prodotti, servizi, processi delle tecnologie dell'informazione, prevista dalla disciplina europea, è ora individuata nell'istituenda Agenzia, la quale viene ad assumere tutte le funzioni in materia di certificazione di sicurezza cibernetica già attribuite al Ministero dello sviluppo economico, comprese quelle relative all'accertamento delle violazioni e all'irrogazione delle sanzioni. Inoltre, ai sensi della lettera *h)* del comma 1 dell'articolo 7 l'Agenzia assume le funzioni in materia di perimetro di sicurezza nazionale cibernetica attribuite alla Presidenza del Consiglio, tra le quali rientrano l'accertamento delle violazioni e l'irrogazione delle sanzioni amministrative, per i soggetti pubblici (nonché i gestori di servizi fiduciari qualificati o di posta elettronica) che facciano parte del perimetro.

Per le finalità di cui al presente decreto, il comma 5 dell'articolo 7 prevede che, nel rispetto delle competenze del Garante per la protezione dei dati personali, l'Agenzia consulta il Garante e collabora con esso, anche in relazione agli incidenti che comportano violazioni di dati personali. Ai sensi del medesimo comma, l'Agenzia e il Garante possono stipulare appositi protocolli d'intenti che definiscono altresì le modalità della loro collaborazione nell'ambito delle risorse disponibili a legislazione vigente e senza nuovi o maggiori oneri per la finanza pubblica.

Segnala inoltre l'articolo 13, che prevede che i trattamenti di dati personali per finalità di sicurezza nazionale, in applicazione del decreto-legge in esame, siano effettuati ai sensi dei commi 2 e 3 dell'articolo 58 del codice in materia di protezione dei dati personali, di cui al decreto legislativo 30 giugno 2003, n. 196. Rammenta a tale proposito che il comma 2 dell'articolo 58 del codice dispone che, ai trattamenti effettuati da soggetti pubblici per finalità di difesa o di sicurezza dello Stato, in base ad espresse disposizioni di legge che prevedano specificamente il trattamento, si applicano: le disposizioni (di cui al comma 1 del medesimo articolo 58) concernenti i controlli relativi ai trattamenti di dati personali effettuati dagli organismi previsti dalla legge 3 agosto 2007, n. 124 (Dipartimento delle informazioni per la sicurezza – DIS, Agenzia informazioni e sicurezza esterna – AISE, Agenzia informazioni e sicurezza interna – AISI) e di dati coperti da segreto di Stato; in base a tali disposizioni (tramite il richiamo all'articolo 160, comma 4, del codice) il componente designato per gli accertamenti dal Garante per la protezione dei dati personali deve prendere visione degli atti e dei documenti rilevanti e riferire oralmente nelle riunioni del Garante; le disposizioni

concernenti la valutazione d'impatto sulla protezione dei dati e la consultazione preventiva del Garante, di cui agli articoli 23 e 24 del decreto legislativo 18 maggio 2018, n. 51, che attua la direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, In particolare l'articolo 23 prevede che, se il trattamento, per l'uso di nuove tecnologie e per la sua natura, per l'ambito di applicazione, per il contesto e per le finalità, presenta un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento, prima di procedere al trattamento, effettua una valutazione del suo impatto sulla protezione dei dati personali. Tale valutazione contiene una descrizione generale dei trattamenti previsti, una valutazione dei rischi per i diritti e le libertà degli interessati, le misure previste per affrontare tali rischi, le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e il rispetto delle norme del citato decreto legislativo n. 51 del 2018. L'articolo 24 del medesimo decreto legislativo prevede invece che il titolare del trattamento o il responsabile del trattamento consultino il Garante prima del trattamento di dati personali che figureranno in un nuovo archivio di prossima creazione se: una valutazione d'impatto indichi che il trattamento presenterebbe un rischio elevato in assenza di misure adottate dal titolare del trattamento per attenuare il rischio; oppure il tipo di trattamento presenti un rischio elevato per i diritti e le libertà degli interessati anche in ragione dell'utilizzo di tecnologie, procedure o meccanismi nuovi ovvero di dati genetici o biometrici; nonché, in quanto compatibili, specifiche ulteriori disposizioni contenute nel medesimo decreto legislativo n. 51 del 2018. Si tratta di quelle relative alle definizioni (articolo 2), ai principi applicabili (articolo 3), al processo decisionale automatizzato relativo alle persone fisiche (articolo 8), agli obblighi del titolare del trattamento (articolo 15), alla protezione dei dati fin dalla progettazione e protezione per impostazione predefinita (articolo 16), al responsabile del trattamento (articolo 18), alla sicurezza del trattamento (articolo 25), all'Autorità di controllo (articolo 37), al diritto al risarcimento (articolo 41), alle sanzioni amministrative (articolo 42) e al trattamento illecito di dati (articolo 43).

Il comma 3 dell'articolo 58 del codice in materia di protezione dei dati personali demanda ad uno o più regolamenti l'individuazione delle modalità di applicazione delle disposizioni in materia di trattamenti di dati personali per fini di sicurezza nazionale o difesa, in riferimento alle tipologie di dati, di interessati, di operazioni di trattamento eseguibili e di persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile, anche in relazione all'aggiornamento e alla conservazione.

L'articolo 16 reca alcune modifiche puntuali alla legislazione vigente conseguenti al nuovo assetto dell'architettura nazionale di cybersicurezza disposta dal decreto in esame. Si tratta principalmente delle modifiche che consentono il passaggio delle competenze in materia di perimetro di sicurezza nazionale dal Dipartimento delle informazioni per la sicurezza e dal Ministero per lo Sviluppo economico all'Agenzia per la cybersicurezza nazionale nonché quelle relative, in particolare, al Centro di Valutazione e Certificazione Nazionale (CVCN) e quelle di competenza dell'Agenzia per l'Italia digitale. Nell'ambito di tali modifiche segnalo in particolare il comma 11 che novella l'articolo 135 del codice del processo amministrativo (di cui al decreto legislativo 2 luglio 2010, n. 104), inserendo tra le ipotesi di competenza funzionale inderogabile del Tribunale amministrativo regionale del Lazio, sede di Roma, anche le controversie aventi ad oggetto i provvedimenti dell'Agenzia per la cybersicurezza nazionale.

L'articolo 17 introduce le disposizioni transitorie e finali. In particolare il comma 1 prevede che, per lo svolgimento delle funzioni ispettive, di accertamento delle violazioni e di irrogazione delle sanzioni, attribuite ai sensi dell'articolo 7 alla neo-

istituita Agenzia per la cybersicurezza nazionale, essa possa avvalersi « dell'ausilio » del personale dell'organo centrale del Ministero dell'interno per la sicurezza e la regolarità dei servizi delle telecomunicazioni, vale a dire del Servizio di polizia postale e delle comunicazioni del Dipartimento della pubblica sicurezza previsto dall'articolo 7-*bis* del decreto-legge 27 luglio 2005, n. 144 del 2005. Il comma 2 dispone che la nascente Agenzia operi « con l'ausilio » del citato organo centrale del Ministero dell'interno, per quanto concerne le funzioni di attuazione e di controllo indicate dall'articolo 5 del decreto-legge n. 105 del 2019 recante disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica e di disciplina dei poteri speciali nei settori di rilevanza strategica. Il comma 3 del medesimo articolo 17 stabilisce che il « personale dell'Agenzia », nello svolgimento delle funzioni ispettive, di accertamento delle violazioni e di irrogazione delle sanzioni, di cui all'articolo 7, nonché delle funzioni relative all'attuazione e al controllo dell'esecuzione dei provvedimenti assunti da parte del Presidente del Consiglio dei ministri ai sensi dell'articolo 5 del citato decreto-legge, rivesta la qualifica di pubblico ufficiale. Tale qualifica ai sensi del successivo comma 4 è attribuita, nello svolgimento delle proprie funzioni, anche al personale dell'Agenzia addetto al *Computer Security Incident Response Team* (CSIRT) Italia, trasferito presso l'Agenzia dall'articolo 7 del decreto-legge in esame. Rammenta che lo CSIRT è una struttura i cui compiti sono definiti dal decreto legislativo 18 maggio 2018, n. 65 e dal decreto del Presidente del Consiglio dei ministri 8 agosto 2019. Tra questi, vi sono: il monitoraggio degli incidenti a livello nazionale; l'emissione di preallarmi, allerte, annunci e divulgazione di informazioni alle parti interessate in merito a rischi e incidenti; l'intervento in caso di incidente; l'analisi dinamica dei rischi e degli incidenti; la sensibilizzazione situazionale.

Come stabilito dal medesimo comma 4 dell'articolo 17, la trasmissione delle notifiche di incidente ricevute dal CSIRT Italia all'organo centrale del Ministero dell'interno per la sicurezza e per la regolarità dei servizi di telecomunicazione costituisce adempimento dell'obbligo di cui all'articolo 331 del codice di procedura penale in materia di denuncia da parte di pubblici ufficiali e incaricati di un pubblico servizio.

Nessuno chiedendo di intervenire, rinvia il seguito dell'esame ad altra seduta.

La seduta termina alle 14.40.